Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 4016 – 4020

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

A Security Model Based on Information Self-feedback

Huang Rongsheng*， Wu renjie

Hebei North University, Zhangjiakou in hebei province 075000, China

Abstract

Based on the intrusion of the trap theory,the data is devied into domain of inforamtion. The information basic units forms decoy honey guides as the basic elements, in accordance with the target sensitivity which comes up at the time of the invasion of the guides, the value of feedback is adjusted, to achieve the critical situation of the units, and the distribution of domain information belonging network is changed through genetic effects. Meanwhile, this paper introduces the concept of domain target coefficients since the establishment of Information-based Self-Feedback model(ISF), the ultimate access to the information domain attacked. Through the experiments in the actual network scene, the results show: it is the only successful model that forecast and feedback the destruction or threaten from the network attack for the inforamtion of the domain, it also has been able to adjust the trapping strategy with self feedback of informaiton, access to the domain data in the network attack.

*Key words:*feedback; security; Trapping; model;domian inforamtion

1.Introduction

Information indicates the degree of a country's comprehensive competitiveness. With the rapid development of network industries, a large number of highly confidential and highly sensitive information exposed in the network storage medium. These documents bearing the individual's profile information, the Government's Planning Information important proof of contract, if the malicious tampering or theft, would have disastrous consequences for society. If we can at minimum cost and efficient information access to the most protective effect has been the focus of security research over thousands of miles[1].

This paper designs and implements a use of information itself from the invasion of information feedback trapping protection model. Proposed that the purpose of network intrusion into their invasion, regardless of content relevant to the content type of type attack. For the content of the relevant type of network intrusion, taken in honeynet (honeynet) distribution of trapping within the data (the bait) to study the sensitivity of the intruder's data, by information from the feedback mechanism to adjust the data

* Corresponding author. Tel.:+8613603306856

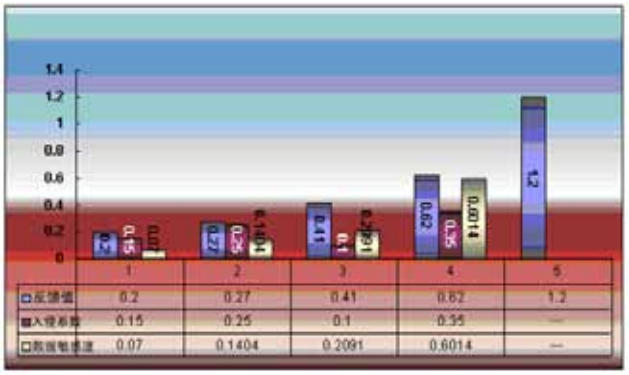
E-mail address: ieee2010@foxmail.com

1877-7058 © 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.

doi:10.1016/j.proeng.2011.08.753

distribution of the honey pot, reduce the scope and precise analysis of the information and, ultimately, the invasion of information the target domain[2].

2.Areas of information planning



	1	2	3	4	5
□反馈值	0.2	0.27	0.41	0.62	1.2
■入侵系数	0.15	0.25	0.1	0.35	—
□防御敏感度	0.07	0.1404	0.2091	0.6014	—

Fig.1 A basic unit example of changes in the value of feedback

Figure 1 shows a trapping system to capture the typical behavior of malicious tampering with documents. Honey trap information to define the subject of primitives, can be learned from Figure 0.2 the initial feedback (information-based element of the initial feedback value is generally less than 0.4). Since the invasion coefficient shows invasion of the user has marked this Honey (primitive operation information on the fall in real terms) were to change data attributes, copy the data, forged content, the remote to accept new data, the final value of the information bounds primitive feedback. The primitive self-feedback information, the intruder left. by the Here, we can get the following conclusion: When the invasion of harmful and destructive behavior increased (the invasion factor is increased), the target sensitivity of geometric trend will increase, while the feedback value of the surge led to the subject of self-excited feedback instinct honey, as protection of data content with the field.

It is worth mentioning that the information in the same field between the base element, the target sensitivity and transmitted with spreading. That individuals within populations are threatened, the population will increase the overall defensive. When the same information within the individual primitive a substantial increase in the value of feedback, there will be more primitive with the domain information as a decoy to attract the intruder object, and ultimately determine whether the target is the invasion of the domain. From the perspective of text classification, the concept of domain refinement than the class much more.

3.Domain information model of self-feedback protection

Relevant to the content-based network intrusion.

Network intrusion mainly through information collection, analysis, sorting after finding the target system vulnerabilities and weaknesses, and in a targeted manner on the target system (server, network equipment and security equipment) invasion and destruction of resources, theft of confidential information, monitor and control activities [1].

We believe that the nature of intrusion by improper means to obtain a legal interest. Is a malicious theft of information (to view, copy, transfer) and damage (altered, deleted). Therefore, the intruder's network attacks can be divided into and the information content related to aggressive behavior and has nothing to

do with the information content of aggressive behavior. particularly for government web portal, according to statistics, 15% of the network data security issues led to destruction of the safety problem caused 18% of the data was compromised. and the current Network security architecture is based on the means to prevent the invasion or the means of intrusion detection, and give up on the invasion of target location.

Definition 13. Data integrity: the integrity of our data integrity and include the contents of the object integrity. Content integrity is the property of the data itself, the content does not change. The object is the data integrity of the service object is not changed. That the contents integrity is a goal-oriented; object is for the integrity of behavior.

Table 1 Invasion of Category

Unrelated to the content-type attack	Relevant to the content type of attack [target sensitivity of the elements]
Exhaustive sexual assault	Copy, copy data
Invasive attacks	Reading, open the data
Denial of service attacks	Delete data
Trojan	Tampering with data
Protocol vulnerabilities	Send or receive data
Buffer overflow attacks	Change the data attributes
Spoofing attack	Create, falsified data

From Table 1 we can see the contents of the usual type of attack is unrelated to the act itself for the invasion; and relevant to the content type of attack is the goal for the invasion. In Table 2 we define the intrusion caused by damage to the contents , and its mathematical description for the invasion factor. invasion of the selection coefficient value is obtained by statistics. We used stand-alone deployment of a virtual honeynet environment, taking into account performance factors, in the other two hosts to deploy the honeypot, and opened based on FTP, HTTP military enthusiasts Portal (12050 arranged trap on the military aspects of honey), and will take legal access will be assumed as the mode of attack, within the campus network measurement system. From June 1, 2008 to 28 June 2008 invasion of the contents of statistics during the day, finally p_i = 1 for the termination conditions, to meet local conditions $p_i \quad p_i \quad m/(m \quad p_i)$, access to a reasonable extent, the intrusion factor shown as Fig.2 and Fig.3.

Table 2 Content-based Attacks and the invasion coefficient table

Illegal operation of intruder on the data	Invasion factor (m)
Copy, copy data	0.25
Reading, open the data	0.20
Delete data	0.50
Tampering with data	0.45
Send or receive data	0.35
Change the data attributes	0.15
Create, falsified data	0.10

Invasion factor, is the intrusion on the extent of damage caused by information content, expressed as m. The feedback from the primitive value of the information and target sensitivity definition, $p_i \quad p_i \quad m/(m \quad p_i)$, where p_i is the original value, $m(p_i - p_i - 1) = p_i^2 \quad p_i \; p_i$ can be deduced that the invasion factor .

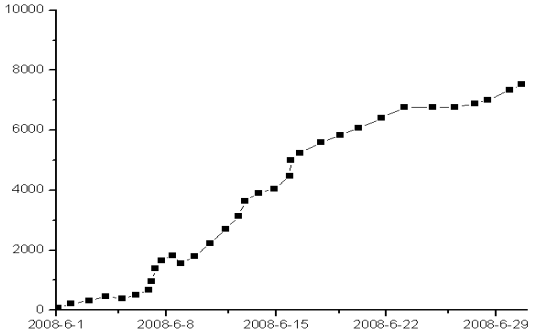


Fig.2 the total number of feedback for one day.

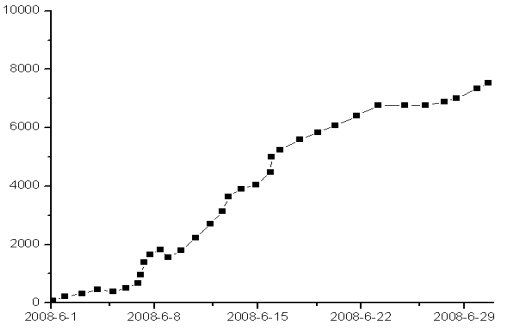


Fig.3 data integrity damage

Since the propagation time in the campus network and scope of the relationship between the primitive trapping occurs within the system of information feedback in a curve on an upward trend in the average distribution. The invasion of these goals through the analysis point of view too. "Intruders" primitive little information delete, distort the operation of the more serious, the majority or the "illegal status" for reading, copying, including downloading behavior.

4.Experimental Analysis

For information on the effectiveness of self-feedback model, we take the field of e-government information as an example. We all levels of government domain gov.cn portal for government class files 123,364 copies, including agricultural economics, business, military defense, policy and institutional research , culture and education, the field of Water six classes total of 50 350 domains. set within the virtual honeynet honeypot trap machine 8. virtual honeynet deployed an average of 350 honey pot field honey trap 20000 standard, accounting for individual 50% of the total number of files, the average distribution of honeypot honey trap standard 2500.

We input the above data, the use of implementation feedback based on information from the security model, from the model of rationality and accuracy of the two aspects of the model is verified. The

accuracy of e-government is used in closed experimental data sets; reasonable of using the campus network based on open experiment.

In order to verify the accuracy of the model, we IBAS and for expansion, which has the goal of targeting the intrusion analysis system (Targeted Invasion Behavior Analysize System, referred to as TIBAS). TIBAS most important feature is that the process of an attack sequence, attack instance itself specific target, ie the demise of the previous attack instances in the scene for the system and are transparent, while, TIBAS able to attack the attack IBAS impact assessment.

IBAS and TIBAS system results in Table 4 which TIBAS experimental data generated by the program statistics for IBAS experimental data, because the system no goal target (the more random attacks), so the feedback on the results correctly determine the require manual analysis and screening.

5.Conclusions

In this paper, based on the theory of network intrusion trapping, combined with knowledge of the natural language understanding, divided by field data and information in the field of primitive as the basic unit of information were furnished to the honey trap honey mark the formation of networks. Meanwhile, according to the honey trap generated by the attack marked the target sensitivity, adjust the value of information-based element of the feedback, so that the information in the genetic effects of primitive place under the guidance of derivatives to adjust the layout of information within the network. We have established a feedback based on information from the protection (Infromation- based Self-Feedback, ISF) model. After intrusion analysis system (Invasion Behavior Analysize System, referred to IBAS) and goal-oriented intrusion analysis system (Targeted Invasion Behavior Analysize System, referred to as TIBAS) of the closed test and the actual campus network experiments show that the attack scenarios: the network model is successfully achieved targets, attacked the field of prediction and prevention; able in a relatively short period of time accurately and quickly adjust the distribution of information policy, access to information within the network domain to be attacked; algorithm has more high autonomy, the composition of the environment from the trap to adjust to the final conclusion stated that rely on models to stand alone to complete.

References

[1] W.E. Ebbers, W.J. Pieterson, H.N. Noordman. Electronic government: Rethinking channel management strategies.Government Information Quarterly 25 (2008) 181–201.

[2] CHEN Feng, LUO Yang-xia, CHEN Xiao-jiang, GONG Xiao-qing, FANG Ding-yi. A survey of the research on network attack technologies. Journal of Northwest University(Natural Science Edition, 2007, 37(2):208-212.

[3] YANG Li,\ZUO Chun,\WANG Yu-Guo. K-Nearest Neighbor Classification Based on Semantic Distance. Journal of Software. 2005, 16(1):2054-2062.

[4] CHU Jun, SU Zhen. E-Government Security Tech. Control. Renmin university press. Beijing, March, 2004.

[5] Michael Clark. Virtual Honeynets. http://online.seciroty focus.com/infocus/1506/, 2001.

[6] Honeynets Projcet. Know Your Enemy: Defining Virtural Honeynets. http://project.honeypots.org/papers/honeynets, 2002.

[7] Anil K. Ghosh. On optimum choice of k in nearest neighbor classification. Computational Statistics and Data Analysis, 2006, 50(11): 3113-31238.

[8] JIANG Zhi-xiong, DING Yue-wei. Network text classification based on K-nearest neighbor method. J. University of shanghai for Science and Technology, 2005, 27(13).